

# Notice of Allowability

Application No.

09/955,165

Applicant(s)

MICHAEL, CHRISTOPH  
CORNELIUS

Examiner

Joseph P. Hirl

Art Unit

2129

## -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to January 17, 2006.
2. ☒ The allowed claim(s) is/are 1,2 and 4-20.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

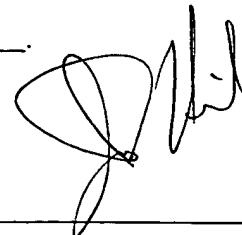
Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

### Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

 P.E.

***Examiner's Amendment***

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

***In the Claims***

2. The claims of the subject application are amended as follows:

1. (Currently amended) A computerized method for detecting anomalous behavior in an executing software program, said method comprising the steps of :

generating a normal execution trace for the software program;

applying a learning algorithm to the normal execution trace to build a finite automaton;

applying an examination algorithm to the finite automaton to identify undesirable transition states in the finite automaton and to create a labeled finite automation; and

applying the labeled finite automaton to an execution trace associated with the executing software program to identify undesirable behavior.

2. (Previously presented) The method of claim 1, wherein application of the learning algorithm occurs during a first learning phase and application of the examination algorithm occurs during a second, examination phase and the learning phase occurs before and independently from the examination phase.

3. (Canceled)

4. (Currently amended) The method of claim 3 1, wherein application of the labeled finite automaton to the execution trace is performed to identify undesirable behavior in a execution trace.

5. (Previously presented) The method of claim 4, wherein the undesirable behavior comprises the undesirable transition.
6. (Previously presented) The method of claim 1, wherein the finite automaton comprises a tuple.
7. (Previously presented) The method of claim 6, wherein the tuple comprises a set of possible states, a set of symbols comprising the input alphabet, a mapping function, a start state, and a set of final states.
8. (Previously presented) The method of claim 6, wherein the tuple comprises a set of states interconnected by labeled transitions.
9. (Previously presented) The method of claim 1, wherein the finite automaton comprises a prefix tree.
10. (Previously presented) The method of claim 9, wherein the prefix tree comprises a plurality of nodes.
11. (Previously presented) The method of claim 10, wherein the plurality of the nodes of the prefix tree correspond to states of the finite automaton.
12. (Previously presented) The method of claim 11, wherein one of the plurality of nodes comprises a root node, with the root node serving as a start state.
13. (Previously presented) The method of claim 12, wherein a remainder of the plurality of nodes comprise accepting states.
14. (Previously presented) The method of claim 10, wherein the learning algorithm selectively merges nodes in the finite automaton.

Art Unit: 2129

15. (Previously presented) The method of claim 1, wherein the learning algorithm comprises a state merging algorithm.
16. (Previously presented) The method of claim 1, further comprising flagging the execution trace associated with the executing software program as malicious if the execution trace associated with the executing software program is rejected by the finite automaton.
17. (Previously presented) The method of claim 1, wherein the execution trace associated with the executing software program is rejected if it does not end in an accepting state.
18. (Currently Amended) The method of claim 3 1, wherein the undesirable behavior comprises at least one of providing an undesired method of entry into the system to unauthorized users, damaging system resources, and elevating user privileges.
19. (Previously presented) The method of claim 1, wherein the finite automaton is built using empirical data.
20. (Previously presented) The method of claim 1, wherein the method is performed by monitoring processes at a system level.

Art Unit: 2129

3. Authorization for this examiner's amendment was given in a fax dated March 28, 2006 from David C. Isaacson.

***Correspondence Information***

4. Any inquiry concerning this information or related to the subject disclosure should be directed to the Primary Examiner, Joseph P. Hirl, whose telephone number is (571) 272-3685. The Examiner can be reached on Monday – Thursday from 6:00 a.m. to 4:30 p.m.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, David R. Vincent can be reached at (571) 272-3080.

Any response to this office action should be mailed to:

Commissioner of Patents and Trademarks,

Washington, D. C. 20231;

Hand delivered to:

Receptionist,

Customer Service Window,

Randolph Building,

401 Dulany Street,

Alexandria, Virginia 22313,

(located on the first floor of the south side of the Randolph Building);

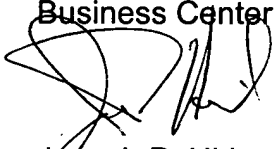
Art Unit: 2129

or faxed to:

(571) 273-8300 (for formal communications intended for entry.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have any questions on access to Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll free).



P.E.  
Joseph P. Hirl  
Primary Examiner  
March 29, 2006